REMARKS

Claims 1-19 are pending. Claims 1-19 are rejected. Claims 9 and 14 are amended. No new subject matter has been added. Claims 1-19 remain pending. Reconsideration of the claims is requested in light of the following remarks.

Claim Rejections - 35 USC § 103

Claims 1-19 are rejected under 35 USC 103(a) as being unpatentable over Gleichauf (US 6,301,668) and further in view of Blanchard (US 6,219,791). The rejection is respectfully traversed.

The Examiner acknowledges that Gleichauf does not teach encrypting a query data packet in accordance with a plurality of encryption keys to product a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability. However, the Examiner states that this is suggested in FIG. 1 and Col. 1, lines 13-15 and 17-20 of Blanchard.

Claim 1 and the other independent claims specify encrypting a query data packet in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability.

There is no suggestion in Blanchard of generating one, much less multiple, encrypted query data packets that include query fields specific to a target vulnerability.

Claim 1 also specifies storing the plurality of encrypted query data packets in a memory. There is nothing in Blanchard that suggests storing a plurality of the previously encrypted query data packets in memory.

Finally, claim 1 specifies scanning the networked computer for a target vulnerability residing therein by sending successive ones of the encrypted-and-stored query data packets to the networked computer and analyzing responses thereto from the networked computer with respect to the characteristic signature. Again there is nothing in Blanchard that remotely suggests sending successive ones of these previously encrypted-and-stored query data packets to networked computers and then analyzing the responses.

The invention as described in the specification and as shown in FIG. 5 explains how pregenerating and storing a plurality of the query data packets and then transmitting the stored plurality of query data packets substantially reduces the amount of time required for generating and encrypting successive packets on the fly. Page 10, line 29 – page 11, line 6.

The invention as specified in the claims solves the precise problem created in the prior art, namely the excessive processing required to generate and encrypt individual query packets one by one on the fly. The invention as specified eliminates this problem by pre-generating and encrypting the query packets in bulk. This feature is not even remotely suggested in Blanchard.
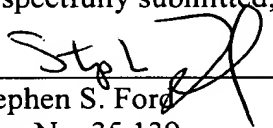
However, to further clarify the patentable subject matter of the invention, claims 9 and 17 have been amended to clarify that the multiple encrypted and stored query packets are transmitted in a batch to the networked computers. This is also clearly not suggested in the cited prior art, and is shown in FIGS. 2 & 5.

Therefore, claims 1-19 are allowable under 35 USC 103(a) over Gleichauf (US 6,301,668) in view of Blanchard (US 6,219,791).

Conclusion

For the foregoing reasons, reconsideration and allowance of claims 1-19 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

Stephen S. Ford
Reg. No. 35,139